NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 1600.1
Effective Date:
November 03, 2004
Expiration Date:
November 03, 2014

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: NASA Security Program Procedural Requirements w/Change 2 (4/01/2009)

Responsible Office: Office of Protective Services

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

Appendix J: NASA Foreign National Visitor Security/Technology Control Plan Sample Template

SECURITY/TECHNOLOGY TRANSFER CONTROL PLAN (STTCP)
FOR

//Name of International Visitor//

PREPARED BY:

//Center IVC, Security Office and Sponsoring Organization//

//CENTER//
//ADDRESS//
//CITY, STATE, ZIP CODE//

//DATE SIGNED AND IMPLEMENTED//

Sponsor Signature	*Security Office Representative*

Foreign National Visitor *Escort (If required)*

SECURITY/TECHNOLOGY CONTROL PLAN

I. INTRODUCTION

This Security/Technology Control Plan (STTCP) has been prepared by the International Visit Coordinator Office (IVC), the Center Security Office, and visit sponsor to ensure that //Type of Technology/// is protected in accordance with NASA policy and procedure, and in accordance with the Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR).

The //Sponsoring Organization// is ultimately responsible for implementation and compliance with the policies set forth in the STTCP.

II. SCOPE

This STTCP covers technical data/know-how to be transferred to //Name of Individual// for tasks associated with //Type of Technology// at //Center// for the period beginning //Month, Day and Year// and ending //Month, Day and Year//. Appendix J(1) contains an overall description of the Program/Project, a description of the tasks to be performed by the Foreign National (FN), a description of technical data (including software), access to hardware (including computers), and know-how to be transferred to the FN in connection with tasks to be performed. Appendix J(2) contains security requirements. Appendix J(3) contains a general briefing on the export control regulations of the State and Commerce Departments and established security requirements for this STTCP.

III. TECHNOLOGY TRANSFER REQUIREMENTS

A. Training Requirements

The //Center// has developed the technology transfer control briefing (see Appendix J(3)) for those individuals on //Program/Project// who shall regularly have contact with //Name of Individual// on the Program/Project. The briefing contains an overview of export regulations. Appendix J(2) contains security and technology transfer requirements (e.g., IT security and interfaces, hours of access, facility access, movement restrictions) as they relate to the //Program/Project Name//. The Center IVC shall maintain a record of all personnel briefed.

B. U.S. Personnel Briefing

1. All U.S. //Center Name// personnel working with //Name of Individual// on the //Program/Project// shall read this plan and sign a Non-Disclosure Statement.

2. All //Program/Project// personnel signing the Non-Disclosure Statement do so by acknowledging that they understand what is required of them with respect to technology transfer and security issues regarding their work with //Name of Individual//. All questions regarding the transfer of technology falling outside the described scope contained in Appendix J(3) of this STTCP, or any questions with regard to what falls within the scope of this STTCP, shall be directed to the Center Export Administrator (CEA). All questions regarding Security Program aspects to include IT Security (Appendix J(2)) of this STTCP shall be directed to the International Visits Coordinator (IVC) or Security Office. In all cases, new personnel working with //Name of Individual// on a regular basis must sign a

Non-Disclosure Statement before they enter the program/project.

C. Foreign Nationals Briefing

1. Any Foreign Nationals (FN) authorized by NASA to be assigned or to work for //Center Name// on the //Program/Project//shall be required to sign a Non-Disclosure Statement.

2. All authorized FN personnel working at //Center Name// on the //Program/Project Name// shall be provided a security/technology transfer control plan (STTCP). The STTCP shall include an oral and written briefing (see Appendix J(3) for written briefing), as well as a description of the task that specifically details the hardware, technology, know-how, data, drawings, software, and information which shall or shall not be exported (divulged) to //Name of Individual//.

IV. PHYSICAL SECURITY

All FN are required to appropriately display their issued NASA Photo-Id badge that identifies them as foreign persons (i.e., Orange Badge for Non-Designated Country Nationals and Red Badge for Designated Country Nationals) at all times while on NASA premises. Security requirements are spelled out in Appendix J(2).

Appendix J

(1) Project Description

In collaboration with the International Visits Coordinator, Security Office, and Center Export Administrator (CEA), Program/Project Managers shall provide a detailed description of the project the FN is to work on, the technology and information to which they are authorized access (transfer), the types of hardware, software and, data they need and have access to, and other pertinent information associated with the visit approval. Sample description is provided below:

Using this data as a constraint, the FN visitor shall, in collaboration with Drs. Jones and Miller, develop simple models of CMEs, which shall be compared to the observations. The known size and orientation of the flux rope at the surface shall be used as a starting point for the simple flux rope models. The model shall be propagated from the Sun and the resulting synthetic coronagraph images computed. The goal is to develop techniques and simple models for the interpretation of data from the STEREO mission. In order to perform these tasks, //Name of Individual// shall need access to technical information that is available in the open literature, a standard PC, and software programs such as IDL and Microsoft Office. These software programs fall under the jurisdiction of the Commerce Department and do not require a license to be exported to //Individuals Country//. //Name of Individual// shall also require access to published SOHO data. All of this work is the level of basic, scientific research, the results of which shall be published in open literature.

The work to be performed and the technical data, hardware and software to be accessed by //Name of Individual// is limited to the specific conditions and restrictions specified in this document. Without approval, //Name of Individual// is not authorized for any other work assignment, and is not authorized for access to any other technical data, hardware or software, or IT system. This STTCP is valid only for the //Program/Project// task specified.

Recordkeeping:

Each NASA employee who transfers controlled information under a license or license exemption must keep appropriate records of their transfers. The records must indicate the following: (1) the exporter (the person transferring the information), (2) date of transfer, (3) recipient, (4) description of the controlled information transferred, (5) title of the document, software program, computer file, etc., (6) method of transfer, and (7) export authorization. The records must be submitted to the IVC.

(2) Security

I. Responsibilities

A. NASA Personnel - All //Name of Center// personnel are responsible for being knowledgeable of all aspect of NASA and //Name of Center// security processes and procedures as they relate to the protection of information, assets, and resources that is entrusted to them as part of their NASA assignment. Specifically, //Name of Center// employees and contractors working on programs requiring access to classified, sensitive, or export controlled data or items, or employees working within controlled areas where classified, sensitive, or export controlled data or items exist or is discussed, must practice due diligence to ensure that the data or items are not exposed to access by any foreign person unless they are aware of a prior approval for that access. In addition, Security shall brief people on what this means during the STTCP briefing. All //Name of Center// personnel who shall have regular contact with the Foreign National addressed by this specific STTCP shall be briefed on and be knowledgeable of the specific restrictions stated in this STTCP.

B. Foreign National - Any Foreign National issued a NASA photo-ID for access to //Name of Center// must be knowledgeable of all aspects of //Name of Center // security processes related to issuing of photo-ID, access control, and internal security procedures. Specifically, the Foreign National must be aware of and comply with all imposed restrictions related to the physical access to the Center, facilities, and controlled areas and visual or audible access to information not approved as part of this STTCP agreement.

C. Foreign National's Host/Supervisor - The //Name of Center// employee who is hosting or supervising a Foreign National for photo-ID access to //Name of Center// must be aware of all security process at //Name of Center// that relate to the protection of information, assets, and resources. Specifically, the host or supervisor of the Foreign National addressed by this specific STTCP shall be briefed on and be knowledgeable of the specific restrictions stated in this documents.

II. Identification

A. All personnel who access //Name of Center// for any purpose other than tours or open house are provided a NASA-photo-ID or visitors pass. This identification must be worn visibly above the waist at all times while accessing and on //Name of Center//. In addition, all personnel are responsible for challenging anyone who is not wearing a NASA photo-ID or //Name of Center// visitor pass, particularly in their work area.

B. Foreign Nationals who are employed by, reside at, or who frequent //Name of Center// on a regular, continuous, and long-term basis are provided an appropriate NASA photo-ID which allows unescorted business hours only access to //Name of Center//. The

NASA photo-ID provided to Foreign Nationals shall be color-coded in accordance with the requirements established in Chapter 7, NPR 1620.1B, NASA Security Procedural Requirements.

C. The NASA photo-ID issued to a Foreign National signifies that the Foreign National has met all security reliability investigation requirements and has negotiated and implemented the appropriate STTCP. All rights and privileges associated with the implementation of the STTCP and issuance of a NASA photo-ID shall expire at the end of the visit approval or at the expiration of the Foreign National's Passport and Visa, whichever is shorter. It is the responsibility of the FN and their host/supervisor to complete the processes necessary to extend the photo-ID and STTCP beyond this date.

D. Upon departure from //Name of Center// for travel to any foreign destination, the FN is required to surrender the photo-ID to the Security Office. The photo-ID shall be returned to the FN upon return from the travel.

III. Controlled Areas

A. For the most part //Name of Center// is considered open and accessible to the general population that is authorized for unescorted access. There are areas which are designated "Security Areas" as part of //Name of Center// requirement to comply with Federal guidelines for the protection of classified information, NASA critical resources, sensitive data and materials, and safety requirements.

B. Unescorted access by Foreign Nationals to any Security Area established to protect classified information is prohibited.

C. Unescorted access by Foreign Nationals to areas where NASA critical resources or sensitive data and materials are protected must be agreed upon approved in writing by the cognizant //Name of Center// employee responsible for the area and Security Office.

D. Unescorted access by Foreign Nationals to the open and general work areas of //Name of Center// other than those the FN is assigned to work is prohibited.

IV. Reporting Requirements

A. All //Name of Center// personnel briefed on the information stated in this STTCP are required to report to the Security Office any deviation from the policies, guidelines, or procedures stated within.

B. In addition, all //Name of Center// personnel are required to report any suspicious or unusual behavior or activity by a FN at //Name of Center//.

(3) Briefing on Export Administration Regulations (EAR) - International Traffic in Arms Regulations (ITAR)

I. Export Administration Regulations (EAR) [15 CFR 730-7741]

The Export Administration Regulations (EAR) are administered by the Commerce Department under the authority granted by the Export Administration Act of 1979 as amended.

Controlled Commodities

Information not controlled under the ITAR shall be controlled by the Commerce

Department. The counterpart to the United States Munitions List of the State Department's ITAAR is the Commerce Control List (CCL) of the Commerce Department's EAR.

Foreign National

The definition of a Foreign National is the same as the definition under the ITAR. It is a person who does not have permanent resident status or is not a protected individual (has not been granted political asylum or has not been granted refugee status.

Technical Data

Specific information necessary for the "development," "production," or "use," of an item specified within the Commodity Control List (CCL).

Publicly Available

Information which has been made available to the public or to a community of persons free or at no more than the cost of reproduction and distribution. This includes information that has been published or place in libraries. It also includes fundamental research in basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly with the scientific community.

Export

An export is a release of commodity, technology, or software to a Foreign National in this country or abroad. An export to a Foreign National in this country is deemed an export to the home country of the Foreign National.

Examples of Commodities Controlled by the CCL

The following is an example directly from the Commerce Department regulations. You shall notice that while the State Department specifies general items that are controlled (e.g., remote sensing satellites), the Commerce Department specifies controlled thresholds for each commodity:

3A001 - Electronic Components - is the general heading under the Export Classification Number (ECCN).

a. 2 EEPROMs, flash memories and SRAMS having any of the following:

- Rated for operation at an ambient temperature above 398K (125 degrees C);
- Rated for operation at an ambient temperature below 218K (-55 degrees C); or
- Rated for operation over the entire ambient temperature range from 218K (-55 degrees C) to 398K (125 degrees C).

If the item in question is controlled because it exceeds the specified thresholds above, the exporter must then determine whether the item is controlled to the specific country of destination. In addition, one or more different exemptions shall be available.

This is just one example from the approximate four hundred pages of commodities and specifications listed under the Commodity Control List (CCL). Each commodity then lists specific controls for those specifications which would apply to certain countries for certain policy reasons (e.g., antiterrorism, missile technology, national security, regional

stability, etc.). Since publication outside NASA would involve all countries, the lowest thresholds would apply. To publish all the parameters would virtually require a republication of the regulations. What follows is an illustrative list, not an exhaustive list, of general commodities, which, depending in the specifications, could be sensitive.

1. Electronics - design, development, and production

a. Integrated circuits
b. Monolithic circuits
c. Hybrid integrated circuits
d. Multichip integrated circuits
e. Film type integrated circuits
f. Optical integrated circuits
g. Field programmable gate arrays
h. Microwave or millimeter wave devices
i. Superconductive electromagnetic amplifiers
j. Space qualified and rad hardened photovoltaic arrays
k. Space qualified magnetic tape recorders
l. Signal analyzers exceeding 31 GHz
m. Spectrometers
n. Vacuum microelectronic devices
o. Hetero-structure semiconductor technology
p. Superconductive devices or circuits

2. Computers

a. High speed digital computers
b. Electronic computers operating at temperature extremes (below -45 deg. C or above 85 deg. C)
c. Equipment designed for image enhancement
d. Specially designed computers for signal processing

3. Information Security

a. Systems, equipment, and software designed or modified to use cryptography.

4. Sensors

a. Certain "space-qualified" focal plan arrays
b. Multispectral imaging sensors
c. Image intensifier tubes

u. Deformable mirrors
e. Lasers
f. "Space-qualified" laser radar and LIDAR equipment
g. Magnetometers

5. Materials

a. Composite structures or laminates
b. Ceramic matrix composite materials
c. Piezoelectric polymers and thin films

Penalties for Failure to Adhere to the EAR

There are both substantial criminal and civil penalties for violations of the EAR. A criminal conviction could lead to fines of up to $1M and 10 years imprisonment. In addition, one could incur civil penalties of up to $100,000. Also, NASA could lose its export privileges.

II. International Traffic in Arms Regulations (ITAR [22 CFR 120 - 130])

Section 38 of the Arms Export Control Act (22 USC 2778) authorizes the President of the United States to control the export and import of defense articles. The Presidential authority to promulgate regulations with respect to the export and import of defense articles was delegated to the Secretary of State by Executive Order 11958. The ITAR implements this delegated authority.

Defense Article

A defense article is any commodity listed on the United States Munitions list (USML) of the ITAR (Section 121.1). Defense articles on this list include all spacecraft including communication satellites, remote-sensing satellites, scientific satellites, research satellites, navigation satellites, experimental and multi-mission satellites as well as ground control stations for those satellites (the DSN). In addition, the list includes all components, parts, accessories, attachments, and associated equipment specifically designed or modified for those remote sensing satellites or the DSN.

Export

Sending or taking a defense article out of the U.S.; or transferring control of a defense article to a Foreign National whether in the U.S. or abroad; or disclosing technical data to a Foreign National whether in the U.S. or abroad.

Foreign National

A Foreign National is anyone who is not a permanent resident or anyone who has not been granted refugee status, or anyone who has not been granted political asylum.

Technical Data

Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes all classified information. Tech data also

includes drawings, blueprints, photographs, instructions, and documentation.

Software

Software includes, but is not limited to, the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis, and repair of a defense article. In addition, software employing cryptographic techniques shall require a license.

Publicly Available

Information which is published and which is generally available to the public. This includes general scientific, mathematical, and engineering principles taught in schools and colleges. It also includes general marketing information on function, purpose, or general system descriptions of defense articles. Additionally, fundamental research in science and engineering, which is ordinarily published and widely disseminated, is also considered to be publicly available.

NASA Exemptions

In addition to general exemptions available to any "exporter," such as publicly available information, there are specific exemptions available to NASA. If there is a signed NASA international agreement with a foreign Governmental body and a NASA Task Order which allows NASA to transfer date to a foreign partner, then such things as operational, repair, assembly, modification, maintenance or test technical data would typically be allowed if the information is properly marked in accordance with the international agreement.

Additionally, controlled "interface" information, even including some design details, could also be sent where there is an international agreement. Interface information means that NASA can exchange design information, with "non-proscribed" countries, as long as the design details are limited to the interface and do not describe sufficient design information to enable the production of the entire component. In addition, the information transferred must be marked in accordance with the international agreement to indicate that the information is being transferred under an exemption (125.4 (b) (3)), is for use exclusively on a particular project and that is not for re-export without the permission of NASA or the State Department.

Additional Examples of Unclassified Defense Articles on the Munitions List

1. Energy conservation devices for producing electrical energy from solar energy or chemical reaction and designed for military use.
2. Infrared focal plane array detectors specifically designed for military use.
3. Infrared, visible, and ultraviolet devices specifically designed for military use.
4. Radar systems specifically designed for military use with capabilities such as:

a. Search
b. Acquisition
c. Tracking
d. Imaging radar systems

5. Command, control and communications systems designed for military use.
6. Computers specifically designed or developed for military use.
7. Inertial platforms and sensors for weapons.
8. Guidance control and stabilization systems.
9. Astro-compasses and star trackers.
10. Accelerometers and gyros designed for military use.
11. Information security systems utilizing cryptographic systems.
12. Photointerpretation, stereoscopic plotting, and photogrammetry specifically designed for
13. military purposes.
14. Solid state devices specifically designed or modified for military use.
15. GPS receivers that employ any of the following:

    a. encryption or decryption capabilities (e.g., Y-Code) of PPS signals;
    b. produce navigation results above 60,000 feet and 1,000 knots velocity or greater;
    c. are designed or modified for use with a null steering antenna designed to reduce or avoid jamming signals or designed or modified for use with unmanned air vehicle systems capable of delivering at least 500 kg payload to a range of at least 300 km. (if less capability but designed for military then captured here).

15. Submersible vessels, manned and unmanned, tethered or untethered, designed or modified for military use.
16. Space launch vehicles and their components, parts, accessories, attachments, and associated equipment. (NO NASA EXEMPTION FOR LAUNCH VEHICLE INTERFACE DATA).
17. Heat shields and components thereof fabricated of ceramic or ablative materials.
18. On-board navigation software which corrects the trajectory and achieves system accuracy of 3.33 percent or less of the range.
19. Structural materials for space launch vehicles such as composite structure, laminates, ceramic, and composite materials.
20. Launch vehicle attitude control equipment.
21. Design technology for shielding or rad hardening of spacecraft electrical circuits and subsystems.

Penalties for Failure to Adhere to the ITAR

There are both substantial criminal and civil penalties for violations of the ITAR. A criminal conviction could lead to fines of up to $1M and 10 years imprisonment for each violation. In addition, one could incur civil penalties of up to $100,000. Also, NASA could lose its privilege to export goods and services.

| TOC | ChangeHistory | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | AppendixA | AppendixB | AppendixC | AppendixD | AppendixE | AppendixF | AppendixG | AppendixH | AppendixI | AppendixJ | AppendixK | AppendixL | AppendixM | AppendixN | AppendixO | ALL |

| NODIS Library | Organization and Administration(1000s) | Search |

DISTRIBUTION:
NODIS